

ISO/TR 12489:2013-11 (E)

Petroleum, petrochemical and natural gas industries - Reliability modelling and calculation of safety systems

Contents		Page
Foreword		v
Introduction		vi
1	Scope	1
2	Analysis framework	2
2.1	Users of this Technical Report	2
2.3	Overview of the reliability modelling and calculation approaches considered in this Technical Report	4
2.4	Safety systems and safety functions	7
3	Terms and definitions	8
3.1	Basic reliability concepts	8
3.2	Failure classification	20
3.3	Safety systems typology	24
3.4	Maintenance issues	25
3.5	Other terms	28
3.6	Equipment-related terms	29
4	Symbols and abbreviated terms	30
5	Overview and challenges	33
5.1	General considerations about modelling and calculation challenges	33
5.2	Deterministic versus probabilistic approaches	35
5.3	Safe failure and design philosophy	35
5.4	Dependent failures	36
5.5	Human factors	37
5.6	Documentation of underlying assumptions	40
6	Introduction to modelling and calculations	41
6.1	Generalities about safety systems operating in "on demand" or "continuous" modes	41
6.2	Analytical approaches	44
7	Analytical formulae approach (low demand mode)	47
7.1	Introduction	47
7.2	Underlying hypothesis and main assumptions	47
7.3	Single failure analysis	48
7.4	Double failure analysis	50
7.5	Triple failure analysis	55
7.6	Common cause failures	56
7.7	Example of implementation of analytical formulae: the PDS method	57
7.8	Conclusion about analytical formulae approach	57
8	Boolean and sequential approaches	58
8.1	Introduction	58
8.2	Reliability block diagrams (RBD)	58
8.3	Fault Tree Analysis (FTA)	59
8.4	Sequence modelling: cause consequence diagrams, event tree analysis, LOPA	61
8.5	Calculations with Boolean models	61
8.6	Conclusion about the Boolean approach	64

9	Markovian approach	65
9.1	Introduction and principles	65
9.2	Multiphase Markov models	68
9.3	Conclusion about the Markovian approach	69
10	Petri net approach	69
10.1	Basic principle	69
10.2	RBD driven Petri net modelling	71
10.3	Conclusion about Petri net approach	74
11	Monte Carlo simulation approach	74
12	Numerical reliability data uncertainty handling	74
13	Reliability data considerations	75
13.1	Introduction	75
13.2	Reliability data sources	76
13.3	Required reliability data	78
13.4	Reliability data collection	80
14	Typical applications	80
14.1	Introduction	80
14.2	Typical application TA1: single channel	82
14.3	Typical application TA2: dual channel	97
14.4	Typical application TA3: popular redundant architecture	110
14.5	Typical application TA4: multiple safety system	119
14.6	Typical application TA5: emergency depressurization system (EDP)	124
14.7	Conclusion about typical applications	135
Annex A (informative) Systems with safety functions		136
Annex B (informative) State analysis and failure classification		146
Annex C (informative) Relationship between failure rate, conditional and unconditional failure intensities and failure frequency		152
Annex D (informative) Broad models for demand mode (reactive) safety systems		160
Annex E (informative) Continuous mode (preventive) safety systems		167
Annex F (informative) Multi-layers safety systems/multiple safety systems		170
Annex G (informative) Common cause failures		173
Annex H (informative) The human factor		180
Annex I (informative) Analytical formulae		186
Annex J (informative) Sequential modelling		207
Annex K (informative) Overview of calculations with Boolean models		213
Annex L (informative) Markovian approach		221
Annex M (informative) Petri net modelling		239
Annex N (informative) Monte Carlo simulation approach		248
Annex O (informative) Numerical uncertainties handling		252
Bibliography		255